

# Cryptology ePrint Archive: Report 2011/377

## Improved Generalized Birthday Attack

*Paul Kirchner*

**Abstract:** Let  $r, B$  and  $w$  be positive integers. Let  $C$  be a linear code of length  $Bw$  and subspace of  $\mathbb{F}_r$ . The  $k$ -regular-decoding problem is to find a nonzero codeword consisting of  $w$  length- $B$  blocks with Hamming weight  $k$ . This problem was mainly studied after 2002. Not being able to solve this problem is critical for cryptography as it gives a fast attack against FSB, SWIFFT and learning parity with noise. In this paper, the classical methods are used in the same algorithm and improved.

**Category / Keywords:** Generalized Birthday Attack, Linearization, Information-Set Decoding, Wagner, Low memory requirement, SWIFFT, FSB, LPN

**Date:** received 11 Jul 2011

**Contact author:** pole kirchner at gmail com

**Available formats:** [Postscript \(PS\)](#) | [Compressed Postscript \(PS.GZ\)](#) | [PDF](#) | [BibTeX Citation](#)

**Version:** 20110712:141431 ([All versions of this report](#))

**Discussion forum:** [Show discussion](#) | [Start new discussion](#)

---

[ [Cryptology ePrint archive](#) ]